

# Economical quantum cloning in any dimension

Thomas Durt,<sup>1</sup> Jaromír Fiurášek,<sup>2,3</sup> and Nicolas J. Cerf<sup>2</sup>

<sup>1</sup>*TONA-TENA Free University of Brussels, Pleinlaan 2, B-1050 Brussels, Belgium*

<sup>2</sup>*QUIC, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*

<sup>3</sup>*Department of Optics, Palacký University, 17. listopadu 50, 77200 Olomouc, Czech Republic*

The possibility of cloning a  $d$ -dimensional quantum system without an ancilla is explored, extending on the economical phase-covariant cloning machine found in [Phys. Rev. A **60**, 2764 (1999)] for qubits. We prove the impossibility of constructing an economical version of the optimal universal cloning machine in any dimension. We also show, using an ansatz on the generic form of cloning machines, that the  $d$ -dimensional phase-covariant cloner, which optimally clones all uniform superpositions, can be realized economically only in dimension  $d = 2$ . The used ansatz is supported by numerical evidence up to  $d = 7$ . An economical phase-covariant cloner can nevertheless be constructed for  $d > 2$ , albeit with a lower fidelity than that of the optimal cloner requiring an ancilla. Finally, using again an ansatz on cloning machines, we show that an economical version of the Fourier-covariant cloner, which optimally clones the computational basis and its Fourier transform, is also possible only in dimension  $d = 2$ .

PACS numbers: 03.67.-a

## I. INTRODUCTION

During the last decade, many promising applications of ideas developed within the framework of quantum information theory, such as quantum cryptography, quantum computing, quantum cloning, and quantum teleportation were implemented experimentally [1, 2, 3, 4, 5]. Although it is not certain whether these spectacular progresses will lead to a practical quantum computer [6] because of the difficulties related to decoherence, quantum cryptography is already a well established and mature technology [1, 7]. Traditionally, quantum key distribution is implemented with two-level quantum systems, usually referred to as qubits. The security of the quantum key distribution (QKD) protocols such as the BB84 protocol [8] is guaranteed by the *no-cloning* theorem [9, 10], which states that the perfect copying (or cloning) of a set of states that contains at least two non-orthogonal states is impossible. It is, however, possible to realize an approximate quantum cloning, a concept introduced in a seminal paper by Bužek and Hillery [11] where a universal (or state-independent) and symmetric one-to-two cloning transformation was introduced for qubits.

The cloning machines can be used as very efficient eavesdropping attacks on the QKD protocols. In this context, it is important to study machines which optimally clone a particular subset of states of the Hilbert space, for example the Fourier-covariant cloning machine, which optimally copies two mutually unbiased bases under a Fourier transform [12], or the phase-covariant cloning machine, which optimally clones all balanced superpositions of the computational basis states [13, 14, 15, 16, 17, 18, 19, 20]. In particular, the optimal Fourier-covariant cloner in two dimensions, is known to provide the most dangerous eavesdropping strategy for the BB84 quantum cryptographic protocol [8], while the phase-covariant and universal cloners respectively play the same role relatively to the Ekert [21] and 6-states

[22, 23] protocols.

In the present paper, we shall concentrate on the one-to-two cloning machines, which produces two copies. In an eavesdropping scenario, one copy is sent to the legitimate receiver while the other one is kept by the eavesdropper. The  $1 \rightarrow 2$  cloning transformation for qudits can typically be expressed as a unitary operation on the Hilbert space of three qudits — the input, a blank copy, and an ancilla. The presence of ancilla significantly affects the experimental implementation of the cloning operation, which becomes more complicated and sensitive to decoherence as it has been shown in a recent NMR realization of optimal universal qubit cloner [2]. These negative effects, which may drastically reduce the achieved cloning fidelity, may significantly be suppressed if an “economical” approach is followed, which avoids the ancilla. The cloning is then realized as a unitary operation on two qudits only: the input and the blank copy. This is obviously much simpler to implement because it requires less qudits and two-qudit gates, and it requires to control the entanglement of a pair of qudits only. It is thus likely to be much less sensitive to noise and decoherence than its three qudit counterpart, a fact that was recently confirmed experimentally [24]. To date, the only  $1 \rightarrow 2$  cloning machine for which an economical realization is known is the phase-covariant qubit cloner due to Niu and Griffiths [13, 25, 26].

The (asymmetric) phase-covariant qubit cloning machine [13] works as follows. During the process, the qubit to be cloned, initially in state  $|\psi\rangle_B$ , is coupled to another qubit which become the second copy and is initially prepared in state  $|0\rangle_E$  (the labels  $B$  and  $E$  refer to the tradition in quantum cryptography according to which the receiver of the key is called Bob and the eavesdropper Eve). Then, the state  $|\psi\rangle_B|0\rangle_E$  undergoes a unitary transformation  $U_{BE}$  such that

$$U_{BE}|0\rangle_B|0\rangle_E = |0\rangle_B|0\rangle_E$$

$$U_{BE}|1\rangle_B|0\rangle_E = \cos\alpha|1\rangle_B|0\rangle_E + \sin\alpha|0\rangle_B|1\rangle_E \quad (1)$$

It can be shown that when the input qubit is in an equatorial state,

$$|\psi\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B + e^{i\phi}|1\rangle_B) \quad (2)$$

the fidelities of Bob's and Eve's clones give

$$\begin{aligned} F_B &= \langle\psi|_B \text{Tr}_E(\rho)|\psi\rangle_B = \frac{1 + \cos\alpha}{2} \\ F_E &= \langle\psi|_E \text{Tr}_B(\rho)|\psi\rangle_E = \frac{1 + \sin\alpha}{2} \end{aligned} \quad (3)$$

where  $\rho = |\Phi_{BE}\rangle\langle\Phi_{BE}|$  and  $|\Phi_{BE}\rangle = U_{BE}|\psi\rangle_B|0\rangle_E$ . These fidelities do not depend on the azimuthal angle  $\phi$ , so that these cloners are called phase-covariant. The special case  $\alpha = \pi/4$  corresponds to the symmetric phase-covariant cloner, which provides two clones of equal fidelity  $F_B = F_E = (2 + \sqrt{2})/4 \approx 0.85$ .

It is worth emphasizing that, excepted for the two qubits which are used to carry the two copies, this transformation does not require any extra qubit (ancilla), and is thus an economical cloning process. In a recent paper, a general, necessary and sufficient, criterion was derived in order to characterize the reducibility of 3-qubit cloners to 2-qubit cloners, and it was concluded that the phase-covariant cloner is the only cloner in dimension  $d = 2$  that admits an economical realization [26]. The goal of the present paper is to further extend this study, and to investigate whether a two-qudit realization exists also for  $d$ -dimensional cloning machines. More generally, we aim at elucidating the connections that exist between the cloners with or without ancillas. We prove a series of no-go theorems for economical one-to-two cloning. In particular, we show that, without an ancilla, it is impossible to realize the (deterministic) optimal universal cloning machine in any dimension  $d$  (Section II), and that an economical implementation of optimal phase-covariant cloners does not exist for dimensions  $d > 2$  (Section III). This latter result relies on some ansatz on the cloning transformation, which is made very plausible by a numerical check up to  $d = 7$ . As a side-result, we also consider the best economical phase-covariant cloner in  $d$  dimensions, which achieves a high fidelity although it does not perform as well as the optimal phase-covariant cloner with an ancilla (Section IV). Moreover, we provide a strong evidence that the optimal cloning of a pair of mutually unbiased bases, or Fourier-covariant cloning, requires an ancilla if  $d > 2$  (Section V). All these results strongly suggest that the Niu-Griffiths phase-covariant qubit cloner [13], which does not require an ancilla, is quite unique among the  $1 \rightarrow 2$  cloning machines.

## II. UNIVERSAL CLONING MACHINES

Let us begin by introducing an isomorphism between completely positive maps  $\mathcal{S}$  and positive semidefinite operators  $S \geq 0$  on the tensor product of input and output

Hilbert spaces,  $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}}$  [27, 28]. Consider a maximally entangled state on  $\mathcal{H}_{\text{in}}^{\otimes 2}$ ,

$$|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d |j\rangle_1 |j\rangle_2, \quad (4)$$

where  $d = \dim(\mathcal{H}_{\text{in}})$ . The map  $\mathcal{S}$  is applied to the subsystem 2, while nothing happens with subsystem 1. The resulting (generally mixed) quantum state is isomorphic to  $\mathcal{S}$  and reads

$$S = \mathcal{I}_1 \otimes \mathcal{S}_2(d|\Phi^+\rangle\langle\Phi^+|). \quad (5)$$

The prefactor  $d$  is introduced for normalization purposes. A trace preserving map satisfies the condition

$$\text{Tr}_{\text{out}}[S] = \mathbb{1}_{\text{in}}. \quad (6)$$

The CP map  $\rho_{\text{out}} = \mathcal{S}(\rho_{\text{in}})$  can be expressed in terms of  $S$  as follows [29],

$$\rho_{\text{out}} = \text{Tr}_{\text{in}}[\rho_{\text{in}}^T \otimes \mathbb{1}_{\text{out}} S], \quad (7)$$

where  $T$  denotes the transposition in the computational basis.

Let us now consider that  $S$  describes the  $1 \rightarrow 2$  cloning transformation of qudits. The output Hilbert space is endowed with tensor product structure,  $\mathcal{H}_{\text{out}} = \mathcal{H}_B \otimes \mathcal{H}_E$ , where the subscripts  $B$  and  $E$  label the two clones (in the framework of quantum cryptography, they label the authorized user's (Bob's) copy and the spy's (Eve's) copy). For each particular input state  $|\psi\rangle$ , we can calculate the fidelity of each clone as follows,

$$\begin{aligned} F_B(\psi) &= \text{Tr}(\psi_{\text{in}}^T \otimes \psi_B \otimes \mathbb{1}_E S), \\ F_E(\psi) &= \text{Tr}(\psi_{\text{in}}^T \otimes \mathbb{1}_B \otimes \psi_E S), \end{aligned} \quad (8)$$

where in labels the input and  $\psi \equiv |\psi\rangle\langle\psi|$  is a short hand notation for a density matrix of a pure state. We are usually interested in the average performance of the cloning machine, which can be quantified by the mean fidelities,

$$F_B = \int_{\psi} F_B(\psi) d\psi, \quad F_E = \int_{\psi} F_E(\psi) d\psi, \quad (9)$$

where the measure  $d\psi$  determines the kind of the cloning machines we are dealing with. Universal cloning machines correspond to choosing  $d\psi$  to be the invariant measure on the factor space  $SU(d)/SU(d-1)$  induced by the Haar measure on the group  $SU(d)$ . The fidelities (9) are linear functions of the operator  $S$ ,

$$F_B = \text{Tr}[SR_B], \quad F_E = \text{Tr}[SR_E], \quad (10)$$

where the positive semidefinite operators  $R_j$  are given by

$$R_B = \int_{\psi} \psi_{\text{in}}^T \otimes \psi_B \otimes \mathbb{1}_E d\psi, \quad R_E = \int_{\psi} \psi_{\text{in}}^T \otimes \mathbb{1}_B \otimes \psi_E d\psi. \quad (11)$$

In case of universal cloning, the integral over  $d\psi$  can be easily calculated with the help of Schur's lemma, and we get, for instance,

$$\begin{aligned} \int_{\psi} \psi_{\text{in}}^T \otimes \psi_B d\psi &= \frac{2}{d(d+1)} (\Pi_{\text{in},B}^+)^{T_{\text{in}}} \\ &= \frac{1}{d(d+1)} [\mathbb{1}_{\text{in}} \otimes \mathbb{1}_B + d \Phi_{\text{in},B}^+]. \end{aligned}$$

Here,  $\Pi^+$  denotes a projector onto symmetric subspace of two qudits,  $d(d+1)/2$  is the dimension of this subspace, and  $T_{\text{in}}$  stands for transposition with respect to the subsystem in.

The optimal symmetric cloning machine  $S$  should maximize the average of mean fidelities  $F_B$  and  $F_E$  [30],

$$F = \frac{1}{2}(F_B + F_E) = \text{Tr}[SR], \quad (12)$$

where  $R = (R_B + R_E)/2$ . The maximum achievable  $F$  is upper bounded by the maximum eigenvalue  $r_{\text{max}}$  of the operator  $R$ . Taking into account the trace-preservation condition (6), we have [29]

$$F \leq dr_{\text{max}}. \quad (13)$$

In the case of the universal and phase-covariant  $1 \rightarrow 2$  cloning machines considered in the present paper this bound is saturated if we use an ancilla as we shall see below.

We have to calculate the eigenvalues of an operator

$$R = \frac{1}{2d(d+1)} (2\mathbb{1}_{\text{in}BE} + d\Phi_{\text{in},B}^+ \otimes \mathbb{1}_E + d\Phi_{\text{in},E}^+ \otimes \mathbb{1}_B), \quad (14)$$

Due to the high symmetry, the operator  $R$  has only three different eigenvalues. One eigenvalue reads  $1/(d(d+1))$  and is  $d^3 - 2d$ -fold degenerate. The other two eigenvalues are each  $d$ -fold degenerate and the corresponding eigenstates lie in the  $2d$ -dimensional subspace spanned by  $|\Phi^+\rangle_{\text{in},B}|k\rangle_E$  and  $|\Phi^+\rangle_{\text{in},E}|k\rangle_B$ , with  $k = 1, \dots, d$ . The  $d$  eigenstates corresponding to the maximum eigenvalue read,

$$|r_{\text{max}}; k\rangle = \sqrt{\frac{d}{2(d+1)}} (|k\rangle_B |\Phi^+\rangle_{\text{in},E} + |k\rangle_E |\Phi^+\rangle_{\text{in},B}), \quad (15)$$

where  $k = 1, \dots, d$ . It is clear that the support of any admissible optimal cloning CP map  $S$  must be the  $d$ -dimensional space spanned by the eigenstates  $|r_{\text{max}}; k\rangle$ . This will be exploited in what follows to prove that it is not possible to implement the cloning transformation in an economic way, i.e. without an ancilla, just by applying (randomly, with probability  $p_l$ ) a two-qudit unitary transformation  $U_l$  to the original state and a blank copy.

If this convex mixture of the unitaries implements optimal cloning transformation which maximizes the fidelity  $F$ , then, by convexity, each unitary  $U_l$  is optimal in a sense that it yields the maximal mean fidelity. Consider

one such unitary  $U$ . The corresponding operator  $S_U$  represents a pure state, since  $S_U$  is obtained by applying  $U$  to a pure state  $|\Phi^+\rangle$ . The question is thus whether there exists a state

$$|S_U\rangle = \sum_{k=1}^d c_k |r_{\text{max}}; k\rangle \quad (16)$$

such that  $S_U = |S_U\rangle\langle S_U|$  satisfies the trace-preservation condition (6). After a simple algebra, the condition  $\text{Tr}_{BE}[S_U] = \mathbb{1}_{\text{in}}$  turns out to be equivalent to

$$\frac{1}{d+1} \sum_{k=1}^d |c_k|^2 \mathbb{1} + \frac{1}{d+1} \sum_{k,l} c_k c_l^* |l\rangle\langle k| = \mathbb{1}. \quad (17)$$

This condition is equivalent to the requirement that the rank-one projector  $|c^*\rangle\langle c^*|$  is proportional to the identity operator, which is clearly impossible for any dimension  $d \geq 2$ . This concludes our proof that the universal  $1 \rightarrow 2$  economical cloning is impossible.

### III. PHASE-COINVARIANT CLONING MACHINES

Let us now investigate the possibility of the economical implementation of phase-covariant cloning machines which clone equally well all balanced superpositions of computational basis states,

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d e^{i\phi_j} |j\rangle.$$

We will proceed similarly as before and first determine the operators  $R_B^{pc}$  and  $R_E^{pc}$ , where the superscript pc indicates states and operators related to phase-covariant cloning. The integration in Eq. (11) is over the  $d$  phases  $\phi_j$ , and we have to evaluate the integral

$$\begin{aligned} \prod_{j=1}^d \int_0^{2\pi} \frac{d\phi_j}{2\pi} \psi_{\text{in}}^T \otimes \psi_B &= \frac{1}{d} \Phi_{\text{in},B}^+ + \frac{1}{d^2} \mathbb{1}_{\text{in}} \otimes \mathbb{1}_B \\ &\quad - \frac{1}{d^2} \sum_{j=1}^d (|jj\rangle\langle jj|)_{\text{in},B}. \end{aligned}$$

In order to determine the subspace that is the support of all possible optimal cloning transformations  $S^{pc}$ , we have to determine the maximum eigenvalue of the operator  $R^{pc} = (R_B^{pc} + R_E^{pc})/2$  and the corresponding eigenstates. We have

$$\begin{aligned} R^{pc} &= \frac{1}{d^2} \mathbb{1}_{\text{in}} \otimes \mathbb{1}_B \otimes \mathbb{1}_E \\ &\quad + \frac{1}{2d} (\Phi_{\text{in},B}^+ \otimes \mathbb{1}_E + \Phi_{\text{in},E}^+ \otimes \mathbb{1}_B) \\ &\quad - \frac{1}{2d^2} \sum_{j=1}^d [(|jj\rangle\langle jj|)_{\text{in},B} \otimes \mathbb{1}_E + (|jj\rangle\langle jj|)_{\text{in},E} \otimes \mathbb{1}_B]. \end{aligned} \quad (18)$$

Taking into account the symmetry properties of the operator  $R^{pc}$ , we can make an ansatz for the eigenstates of  $R^{pc}$  which correspond to the maximum eigenvalue,

$$|r_{\max}^{pc}; k\rangle = \alpha(|\Phi^+\rangle_{\text{in},B}|k\rangle_B + |\Phi^+\rangle_{\text{in},E}|k\rangle_B) + \beta|kk\rangle_{\text{in},BE}, \quad (19)$$

where  $k = 1, \dots, d$ , and

$$\frac{\alpha}{\beta} = -\frac{\sqrt{d}}{4}(d+2+\sqrt{d^2+4d-4}). \quad (20)$$

One can easily verify that  $|r_{\max}^{pc}; k\rangle$  is indeed an eigenstate of  $R^{pc}$  if the condition (20) is satisfied. However, it is much more difficult to prove that it is the eigenstate with highest eigenvalue and that the  $d$  states (19) are the *only* eigenstates with this maximum eigenvalue. While we have not been able to prove this analytically for arbitrary  $d$ , we have checked numerically that this is indeed the case for  $d = 2, 3, \dots, 7$  and we conjecture that this holds for any  $d$ .

We can now prove that for  $d > 2$  it is not possible to design an economical phase-covariant cloning machine which does not require an ancilla. If such a machine would exist, then there would be a state

$$|S^{pc}\rangle = \sum_{k=1}^d c_k |r_{\max}^{pc}; k\rangle, \quad (21)$$

which would satisfy the trace-preservation condition (6). On inserting (19) into (21) we obtain

$$\begin{aligned} \text{Tr}_{BE}(|S^{pc}\rangle\langle S^{pc}|) &= 2d^{-1} \sum_k |c_k|^2 \mathbb{1} + \gamma \sum_k |c_k|^2 |k\rangle\langle k| \\ &\quad + 2\frac{\alpha^2}{d} \sum_{j \neq k} c_k c_j^* |j\rangle\langle k|, \end{aligned} \quad (22)$$

where

$$\gamma = \beta^2 + \frac{4\alpha\beta}{\sqrt{d}} + \frac{2\alpha^2}{d}.$$

We have to distinguish two cases. If  $\gamma = 0$  then the trace-preservation condition (6) can be satisfied by setting  $c_k = 0$  if  $k \neq l$  and  $c_l = \sqrt{d/2}$  for some  $l \in \{1, \dots, d\}$ . From  $\gamma = 0$  we obtain  $\alpha/\beta = -\sqrt{d}(4 \pm 2\sqrt{2})/4$ . By comparing this expression with Eq. (20) we obtain an equation for  $d$  which has only one positive integer solution  $d = 2$ . In this particular case, the pure state  $|r_{\max}^{pc}; k\rangle$  describes the symmetric Niu-Griffiths phase-covariant cloning machine for qubits [13] and we have, in accordance with Eqs. (1,5),

$$|S^{pc}\rangle = |0\rangle_{\text{in}}|00\rangle_{BE} + \frac{1}{\sqrt{2}}|1\rangle_{\text{in}}(|01\rangle + |10\rangle)_{BE}.$$

For  $d > 2$  it holds that  $\gamma \neq 0$  and the trace-preservation condition thus implies  $c_k c_j^* = C \delta_{jk}$ , where  $C > 0$  is some constant. It is clear that this latter constraint

does not admit any solution, hence we conclude that for  $d > 2$  the economical phase-covariant cloning machine does not exist. Strictly speaking, our proof holds only for  $d = 3, \dots, 7$  where we numerically verified that the eigenstates (19) are the only ones corresponding to the maximal eigenvalue of  $R^{pc}$ , however, we expect that it holds for any  $d > 2$ .

#### IV. SUBOPTIMAL ECONOMICAL PHASE-COVARIANT CLONING MACHINES

Since the optimal phase-covariant cloning cannot be realized without an ancilla, we can ask what is the best economical approximation to the optimal cloner, i.e., which unitary operation on the Hilbert space of two qudits, an input and a blank copy, achieves the maximum cloning fidelity. In our formalism, the unitary operation is represented by a rank one operator  $S_U = |S_U\rangle\langle S_U|$  which satisfies  $\text{Tr}_{AB}[|S_U\rangle\langle S_U|] = \mathbb{1}_{\text{in}}$ . The optimal  $U$  can be easily determined if we impose some natural constraints on the cloning transformation. First of all, we require that it should be invariant with respect to swapping the two clones  $A$  and  $B$ , which implies that the output Hilbert space of  $S_U$  should be the symmetric subspace of the two qudits, spanned by the states  $|kl^+\rangle$  defined as  $|kl^+\rangle = (|kl\rangle + |lk\rangle)/\sqrt{2}$ ,  $k \neq l$ , and  $|kk^+\rangle = |kk\rangle$ . The second condition is that the cloning should be phase covariant, i.e. the map  $S_U$  should be invariant with respect to an arbitrary phase shift applied to the input qubit, followed by the inverse phase shifts on the two clones. Mathematically, this condition can be expressed as

$$[V_{\text{in}}(\phi) \otimes V_B^\dagger(\phi) \otimes V_E^\dagger(\phi)]|S_U\rangle = e^{i\phi}|S_U\rangle, \quad (23)$$

where  $\phi$  is some overall phase factor,

$$V(\phi) = \sum_{k=1}^d e^{i\phi_k} |k\rangle\langle k|,$$

and the phases  $\phi_k$  can be arbitrary. In order to satisfy the condition (23), the state  $|S_U\rangle$  must have one of the following forms

$$\begin{aligned} |S_U\rangle &= |k\rangle_{\text{in}}|lm^+\rangle_{BE}, & k \neq l \neq m, \\ |S_U\rangle &= |k\rangle_{\text{in}}|ll^+\rangle_{BE}, & k \neq l, \\ |S_U\rangle &= \sum_{k=1}^d s_k |k\rangle_{\text{in}}|kl^+\rangle_{BE}. \end{aligned}$$

It is clear that the trace preservation condition can be satisfied only by the third option, provided that  $s_k = e^{i\theta_k}$ . The fidelity of the clones produced by this map is given by

$$F = \frac{1}{2d^2}(d-1 + |\sum_{k \neq l} e^{i\theta_k} + \sqrt{2}e^{i\theta_l}|^2)$$

and is maximized when  $\theta_k = 0$ ,  $k = 1, \dots, d$ . The optimal economical phase-covariant cloning transformation which is invariant with respect to the swapping of the two clones and is also phase covariant can be thus expressed as

$$|k\rangle \rightarrow |kl^+\rangle,$$

where  $l \in \{1, \dots, d\}$  is arbitrary, and the corresponding fidelity reads

$$F_U = \frac{1}{2d^2} [d - 1 + (d - 1 + \sqrt{2})^2].$$

## V. FOURIER-COVARIANT CLONING MACHINES

Although it is not always easy to prove analytically or numerically that certain cloning machines optimize given quantities (like Bob and Eve's fidelities), an educated guess is often possible. For instance, one can show that the overwhelming majority of optimal 1 to 2 cloning machines that can be found in the literature obeys [31] the ansatz given in Refs. [32, 33]. According to this ansatz, the cloning transformation is represented by a pure state in a  $d^4$  dimensional space spanned by the qudits conventionally labeled by  $A$ ,  $B$ ,  $E$  and  $M$  where  $A$  represent Alice's qudit and is formally equivalent to the label  $in$  introduced in the previous section,  $B$  and  $E$  represent Bob's and Eve's qudits as before, while  $M$  represents an external ancilla. Moreover, the cloning state is assumed to be biorthogonal in the Bell bases, where the  $d^2$  qudit Bell states are defined as follows:

$$|B_{m,n}\rangle_{1,2} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \gamma^{kn} |k\rangle_1 |k+m\rangle_2 \quad (24)$$

where  $m, n \in \{0, 1, \dots, d-1\}$ ,  $\gamma$  is the  $d$ -th root of unity, and  $|j\rangle_{1(2)}$  represents a state of the qudit system 1 (2) chosen in the computational basis. They are maximally entangled states and form an orthonormal basis of the  $d^2$ -dimensional Hilbert space of qudits 1 and 2. Because the cloning state is biorthogonal in the Bell bases, it can be expressed as follows:

$$|\Psi\rangle_{A,B,E,M} = \sum_{m,n=0}^{d-1} a_{m,n} |B_{m,n}\rangle_{A,B} |B_{m,-n}\rangle_{E,M} \quad (25)$$

Here  $a_{m,n}$  is a (normalized)  $d \times d$  matrix. The specification of the  $d^2$  amplitudes  $a_{m,n}$  defines the cloning transformation. We now give several examples.

The optimal universal (generally asymmetric) cloning machine is defined by the following amplitude matrix,

$$a_{m,n}^U = x_1 \delta_{m,0} \delta_{n,0} + x_3 \quad (26)$$

The optimal *symmetric* universal  $d$ -dimensional cloner (the one for which Eve's fidelity is maximal, under the constraint that Bob's fidelity is equal to Eve's fidelity) is

obtained by choosing  $x_1^2 = x_3^2 = d/[2(d+1)]$ . It clones all states with the same fidelity, and we recover the standard formula for the fidelity of universal cloners [32, 33, 35, 36]  $F = (3+d)/[2(1+d)]$ .

The qubit phase covariant cloner copies equally well two mutually unbiased qubit bases (maximally-conjugate or mutually unbiased bases are such that any basis state in one basis has equal squared amplitudes when expressed in any other basis). As far as we presently know, the most dangerous attack on the BB84 [8] and Ekert's [21] protocols requires Eve to make use of such a cloner. It possesses two interesting generalizations in higher dimension: (a) the phase-covariant cloner and (b) the Fourier-covariant cloner.

(a) The phase-covariant cloner has already been defined in the previous section; it clones equally well all balanced superpositions of computational basis states,  $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^d e^{i\phi_j} |j\rangle$ . The asymmetric phase-covariant cloning machine is described (for arbitrary dimension) in Ref. [19] (and the symmetric one in [17]). It is defined by the following amplitude matrix:

$$a_{m,n}^{PC} = x_1 \delta_{m,0} \delta_{n,0} + x_2 \delta_{m,0} + x_3 \quad (27)$$

where  $x_1$ ,  $x_2$  and  $x_3$  are real positive parameters. It constitutes the most dangerous currently known attack on  $d$ -dimensional generalizations of Ekert's protocol.

(b) The Fourier-covariant cloner clones equally well two mutually unbiased bases that are discrete Fourier transforms of each other [12]. It constitutes the most dangerous attack on  $d$ -dimensional generalizations of the BB84 protocol. The Fourier cloner is characterized by the following amplitude matrix [34],

$$a_{m,n}^F = x_1 \delta_{m,0} \delta_{n,0} + x_2 (\delta_{m,0} + \delta_{n,0}) + x_3, \quad (28)$$

where  $x_1$ ,  $x_2$  and  $x_3$  are real positive parameters.

It is legitimate to ask whether or not an economic realization of such an optimal cloning machine is possible, so to say whether it is possible to reach the same fidelity without making use of the ancilla. Concretely, this means that it is possible to find  $l_{\max}$  probabilities  $p_l$  and  $l_{\max}$  unitary transformations  $U_{BE}^l$  that act on the qudits  $B$  and  $E$  only such that:

$$S_{ABE} = \text{Tr}_M \Psi_{A,B,E,M}^{opt} = \sum_{l=1 \dots l_{\max}} p_l \Phi_{A,B,E}^l, \quad (29)$$

where  $\Psi = |\Psi\rangle\langle\Psi|$  and  $\Phi = |\Phi\rangle\langle\Phi|$  are short-hand notations for density matrices of pure states, and

$$|\Phi\rangle_{A,B,E}^l = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A U_{BE}^l |k\rangle_B |\psi_0\rangle_E. \quad (30)$$

As a consequence of the convexity of the average fidelity of cloning, if the CP map  $S_{ABE}$  represent an optimal cloning transformation then each unitary transformation  $\Phi_{A,B,E}^l$  is also optimal in a sense that it maximizes the

average cloning fidelity. The support of the CP map  $S$  associated with the cloning machines that fulfill the ansatz (25) is spanned by the  $d$  states

$$|r_p\rangle = {}_M\langle p| \sum_{m,n=0}^{d-1} a_{m,n} |B_{m,n}\rangle_{A,B} |B_{m,-n}\rangle_{E,M}, \quad (31)$$

where  $p \in \{0, 1, \dots, d-1\}$ . In what follows we assume that the states  $|\xi_p\rangle$  are eigenstates with maximum eigenvalue  $r_{\max}$  of an operator  $R$  which appears in the formula for the cloning fidelity,  $F = \text{Tr}[RS_{ABE}]$ . Moreover, we assume that the states  $|r_p\rangle$  are the complete set of eigenstates with the eigenvalue  $r_{\max}$ . Our results obtained in the previous sections reveal that this is true for a symmetric universal cloning machine for any  $d$  and for phase covariant cloning machine for  $d = 2, \dots, 7$ . Here we conjecture that this holds for phase covariant cloning machine and for the Fourier cloner for arbitrary  $d$ .

If economical optimal cloning is possible, we must be able to construct the pure states  $|\Phi\rangle_{A,B,E}^l$  which appear in Eqs. (29) and (30) as linear combinations of the states  $|r_p\rangle$ . This means that there must exist  $dl_{\max}$  amplitudes  $\alpha_k^l$  (with  $\sum_{k=0}^{d-1} |\alpha_k^l|^2 = 1$ ) such that

$$U_{BE}^l |k\rangle_B |\psi_0\rangle_E = \sum_{m,n,j=0}^{d-1} \alpha_{j+m}^l a_{m,n} \gamma^{n(k-j)} |k+m\rangle_B |j\rangle_E, \quad (32)$$

for  $l = 1, \dots, l_{\max}$ . The constraints (32) are a necessary condition for the existence of economical cloning, whenever the support of the admissible CP maps  $S^l$  associated to the economical cloning transformations  $U^l$  is spanned by the  $d$  states  $|r_p\rangle$ .

Let us assume that the optimal cloning state is given by Eq. (25) with the amplitude matrix (28), this includes the whole class of symmetric and asymmetric universal and Fourier-covariant cloning machines. If an economical realization of such cloners exists, then there must exist  $d$  amplitudes  $\alpha_k$  and a unitary transformation  $U_{BE}$  which satisfy Eq. (32). On inserting the explicit formula (28) for the amplitude matrix  $a_{m,n}$  into Eq. (32) we obtain,

$$U_{BE} |k\rangle_B |\psi_0\rangle_E = \sum_{j,m=0}^{d-1} \alpha_{m+j} [x_1 \delta_{m,0} + dx_3 \delta_{j,k} + x_2 (d\delta_{m,0} \delta_{j,k} + 1)] |m+k\rangle_B |j\rangle_E. \quad (33)$$

Unitarity (or equivalently trace preservation (6)) imposes the following condition:

$${}_B\langle k'|_E \langle \psi_0| U_{BE}^\dagger U_{BE} |k\rangle_B |\psi_0\rangle_E = \delta_{k,k'} \quad (34)$$

Taking  $k = k'$  in Eqs. (33) and (34) we get after some algebra

$$\sum_j |\alpha_j|^2 f_d(x_1, x_2, x_3) + |\alpha_k|^2 g_d(x_1, x_2, x_3) = 1, \quad \forall k, \quad (35)$$

where  $f_d$  and  $g_d$  are second order polynomials in  $x_j$ ,

$$\begin{aligned} f_d &= x_1^2 + dx_2^2 + d^2 x_3^2 + 2x_1 x_2 + 2dx_2 x_3 \\ g_d &= (d^2 + 2d)x_2^2 + 2dx_1 x_2 + 2dx_1 x_3 + 2d^2 x_2 x_3. \end{aligned} \quad (36)$$

If we now consider the case  $k \neq k'$  in Eq. (34) we obtain

$$\begin{aligned} & (dx_2^2 + 2x_1 x_2 + 2dx_2 x_3) \sum_j \alpha_j \alpha_{j+k-k'}^* \\ & + dx_2^2 (\alpha_k \alpha_{2k-k'}^* + \alpha_{2k'-k} \alpha_{k'}^*) + 2dx_1 x_3 \alpha_{k'} \alpha_k^* = 0 \end{aligned} \quad (37)$$

Normalization of the cloning state (25) imposes that  $f_d + g_d/d = 1$ . In virtue of Eq. (35), either  $|\alpha_k|^2 = 1/d$ ,  $\forall k$  or  $g_d = 0$ . The latter constraint is neither satisfied by the universal nor by the Fourier-covariant cloners so that in order that such cloners admit an economical realization,  $|\alpha_k|^2 = 1/d$  and the norms of all the  $d$  a priori unknown parameters  $\alpha_k$  must be equal. In order to ensure unitarity, it is still necessary to fulfill the condition (37). It is worth noting that in (37) appear only products of  $\alpha_i^*$  and  $\alpha_j$  the indices of which differ by the same quantity  $i - j = k - k'$ . Hence, if we make the substitution  $k' = k - m$  in Eq. (37) and then sum over  $m = 0, \dots, d-1$ , we get the following constraint,

$$g_d(x_1, x_2, x_3) \sum_j \alpha_j \alpha_{j+m}^* = 0, \quad m \neq 0.$$

Since  $g_d = 0$  is never satisfied by the optimal universal and/or Fourier-covariant cloners, we find that  $\sum_j \alpha_j \alpha_{j+m}^* = 0$ ,  $m \neq 0$ . As a consequence, the satisfaction of the condition (37) also implies

$$x_2^2 (\alpha_k \alpha_{2k-k'}^* + \alpha_{2k'-k} \alpha_{k'}^*) + 2x_1 x_3 \alpha_{k'} \alpha_k^* = 0. \quad (38)$$

In the case of the universal cloner,  $x_2 = 0$  and  $x_1 x_3 \neq 0$  and it is clear that no solution exists for the system for any  $d \geq 2$ .

When the cloner is the optimal Fourier-covariant cloner, it can be shown that the ancilla does not bring extra information about the state under copy, which is expressed by the relation  $x_2^2 = x_1 x_3$ . The amplitudes  $\alpha_j$  must then obey the relations

$$\alpha_k \alpha_{2k-k'}^* + \alpha_{2k'-k} \alpha_{k'}^* + 2\alpha_{k'} \alpha_k^* = 0, \quad \forall k \neq k'. \quad (39)$$

We shall show that this system of equations admits a solution only in dimension  $d = 2$ . This solution corresponds to the (qubit) phase covariant cloner and, in the symmetric case, to the symmetric Niu-Griffiths economical realization already mentioned in a previous section (see also Ref. [26]). The asymmetric economical realization was studied in detail in the reference [26].

Since all the amplitudes  $\alpha_j$  have the same norm, the triangular inequality together with Eq. (39) implies that

$$\alpha_k \alpha_{k+m}^* = \alpha_{k-2m} \alpha_{k-m}^* = -\alpha_{k-m} \alpha_k^*. \quad (40)$$

It is convenient to consider normalized amplitudes  $\tilde{\alpha}_j = \sqrt{d}\alpha_j$ ,  $|\tilde{\alpha}_j| = 1$ . Taking  $m = 1$  we obtain from Eq. (40) the recurrence formula  $\tilde{\alpha}_{k+1} = -\tilde{\alpha}_k^2 \tilde{\alpha}_{k-1}^*$ . Without loss of generality, we can assume  $\tilde{\alpha}_0 = 1$  and express all  $\tilde{\alpha}_j$  in terms of  $\tilde{\alpha}_1$  as follows:  $\tilde{\alpha}_{2n} = (-1)^n \tilde{\alpha}_1^{2n}$  and  $\tilde{\alpha}_{2n+1} = (-1)^n \tilde{\alpha}_1^{2n+1}$ . Substituting these expressions in the constraint  $\sum_{l=0}^{d-1} \alpha_j \alpha_{j+m}^* = 0$  with  $m = 2$  leads to  $\tilde{\alpha}_1^2 = 0$ , which contradicts the fact that  $|\tilde{\alpha}_1| = 1$ . It is only in dimension 2 that the contradiction can be avoided because  $m = 2 = 0$  modulo  $d$  in dimension 2.

The treatment of the phase-covariant cloner (symmetric and asymmetric as well) presents many similarities with the treatment of the symmetric phase-covariant cloner already discussed in the Section II, excepted that the parametrization is different: when the constraints 27 and 32 are satisfied, it is easy to derive the following system of equations:

$$\begin{aligned} x_1^2 + d^2 x_3^2 + |\alpha_k|^2 (g_d - 2dx_2^2) &= 1, & \forall k, \\ 2dx_1 x_3 \alpha_{-k}^* \alpha_k &= 0; & \forall k \neq k' \end{aligned} \quad (41)$$

The solution of the second constraint is  $\alpha_k = \delta_{k,l}$ . Inserting in the first constraint, we get the equation  $x_1^2 + d^2 x_3^2 = 1$  which is fulfilled in dimension  $d = 2$  only, in virtue of the identity  $x_3^2 = (x_1 + x_2 + x_3)(x_2 + x_3)$ , and of the normalization of the cloning state  $x_1^2 + d^2 x_3^2 + dx_2^2 + 2x_1 x_2 + 2x_1 x_3 + 2d x_2 x_3 = 1$ , in which case we recover the Fourier-covariant cloner and its Niu-Griffiths economical realization already mentioned in the section 2. Note that our proof constitutes a strong evidence of the impossibility of economical phase-covariant cloning in any finite dimension different from 2, in agreement with the strict proof of the section IIIB for dimensions 3 to 7. Note also that the 2 dimensional realization of the phase-covariant cloner (27) differs, in our parametrization, from the 2 dimensional Fourier covariant cloner (28), but they can be shown to be equivalent up to a change of basis and to a relabeling of the  $x$  parameters.

## VI. CONCLUSIONS

In this paper, we have focused on one-to-two cloning machines in arbitrary dimensions, and have investigated the connections between the cloners with and without ancillas. We have established a series of no-go theorems for economical cloning, some of them being firm (universal cloner), some others relying on an ansatz which was only tested numerically (phase-covariant and Fourier-covariant cloners). Note that, in our approach, the figure of merit is the cloning fidelity, but it seems that the cloners that optimize Eve's information also fulfill the ansatz (25). In this case, the CP map approach is not very well adapted because of the non-linearity of the information measure. Nevertheless, we were able to establish the validity of the condition (29) in an independent manner, under the assumption of optimality of the ansatz only.

Our results strongly suggest that the Niu-Griffiths economical phase-covariant cloning machine for qubits is quite unique among the optimal  $1 \rightarrow 2$  cloning machines. This conclusion is of importance in connection with the security of quantum cryptographic protocols because it shows that the realization of cloning attacks on quantum cryptographic protocols that exploit higher-dimensional Hilbert spaces would require the mastering and control of three-qudit transformations, which constitutes a serious technological challenge. Another possibility would be of course to implement a sub-optimal economical phase-covariant cloner, as presented in Section IV, but the resulting attack would be weaker.

To be complete, it is worth noting that in the limit of an infinite dimension, the optimal phase-covariant, Fourier-covariant, and universal cloners tend all to a fidelity of  $1/2$ , for which an economical realization exists: the original qudit is replaced by noise with probability  $1/2$  and directed to Eve, or it is resent to Bob without disturbance while Eve gets noise. In this rather trivial limit, economical cloning is always possible, and extremely cheap!

In a future work, it would be interesting to study the possibility of economical one-to-N cloning, where it seems that the limitations are less drastic than in the one-to-two case. For instance the one-to-three and one-to-N cloners studied in [37, 38, 39] also admit an economical realization.

*Note added:* A related work on economical quantum cloning has been reported independently by the QUIT group in Pavia [39], following discussions we had during a visit of the QUIT group in January 2004 which also led to the present paper.

## Acknowledgments

Special thanks to Helle Bechmann-Pasquinucci (QUIT group, University of Pavia), who is partially at the origin of this work, and to the other members of the QUIT group for stimulating discussions. TD is a Postdoctoral Fellow of the Fonds voor Wetenschappelijke Onderzoek-Vlaanderen. This research was supported by the Belgian Office for Scientific, Technical and Cultural Affairs in the framework of the Inter-University Attraction Pole Program of the Belgian government under grant V-18, the Fund for Scientific Research - Flanders (FWO-V), the Concerted Research Action "Photonics in Computing", the Solvay Institutes for Physics and Chemistry, and the research council (OZR) of the VUB. NJC and JF acknowledge financial support from the Communauté Française de Belgique under grant ARC 00/05-251, and from the EU under projects RESQ (IST-2001-37559) and CHIC (IST-2001-33578). JF also acknowledges support from the grant LN00A015 of the Czech Ministry of Education.

- 
- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
  - [2] H-K Cummins, C. Jones, A. Furze, N-F Soffe, M. Mosca, J. Peach and J-A Jones, *Phys. Rev. Letters* **88**, 187901 (2002).
  - [3] N. Gisin, I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, *Nature (London)* **421**, 509 (2003).
  - [4] J. Du *et al.*, *Phys. Lett. A* **302**, 229 (2002).
  - [5] S. Gulde, M. Riebe, G. P-T Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, R. Blatt, *Nature (London)* **421**, 48 (2003).
  - [6] J. Jones, *Nature (London)* **421**, 29 (2003).
  - [7] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf and P. Grangier, *Nature (London)* **421**, 238 (2003).
  - [8] C. H. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984) p. 175.
  - [9] D. Dieks, *Phys. Lett. A* **92**, 271 (1982).
  - [10] W.K. Wootters and W.H. Zurek, *Nature (London)* **299**, 802 (1982).
  - [11] Buzek, V., and Hillery, *Phys. Rev. A* **54**, 1844 (1996).
  - [12] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002); M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, *J. Phys. A* **35**, 10065 (2002).
  - [13] C-S. Niu and R.B. Griffiths, *Phys. Rev. A* **60**, 2764 (1999).
  - [14] D. Bruss, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, *Phys. Rev. A* **62** 012302 (2000).
  - [15] N. J. Cerf, T. Durt, and N. Gisin, *J. Mod. Opt.* **49** 1355 (2002).
  - [16] H. Fan, K. Matsumoto, X.-B. Wang, and M. Wadati, *Phys. Rev. A* **65**, 012304 (2002).
  - [17] H. Fan, H. Imai, K. Matsumoto and X.B. Wang, *Phys. Rev. A*, **67**, 022317 (2003).
  - [18] A. T. Rezakhani, S. Siadatnejad, A. H. Ghaderi, quant-ph/0312024.
  - [19] T. Durt, D. Kaszlikowski, J-L Chen, and L-C Kwek, *Phys. Rev. A* **69**, 032313 (2004).
  - [20] L.-P. Lamoureux and N.J. Cerf, *Quant. Inform. Comp.* **5**, 32 (2005).
  - [21] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
  - [22] D. Bruss *Phys. Rev. Lett.* **81**, 3018 (1998).
  - [23] H. Bechmann-Pasquinucci and N. Gisin, *Phys. Rev. A* **59**, 4238 (1999).
  - [24] J-F Du, T. Durt, P. Zou, L-C Kwek, C-H Lai, C-H Lo and A. Ekert, quant-ph/0311010 (2003).
  - [25] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, *Phys. Rev. A* **56**, 1163 (1997).
  - [26] T. Durt and J. Du, *Phys. Rev. A* **69**, 062316 (2004).
  - [27] A. Jamiolkowski, *Rep. Math. Phys.* **3**, 275 (1972).
  - [28] M.-D. Choi, *Linear Algebr. Appl.* **10**, 285 (1975).
  - [29] J. Fiurášek, *Phys. Rev. A* **64**, 062310 (2001).
  - [30] J. Fiurášek, *Phys. Rev. A* **67**, 052314 (2003).
  - [31] The deep reason for the appearance of Bell states in the formalism of cloning machines is the existence of an underlying group of symmetry, the discrete Heisenberg-Weyl group. In a paper in preparation, the role of a cyclic subgroup of this group will be analyzed in details. It will be shown that some restrictive assumptions must be made about the optimality of the cloner (see also [19]). The validity of the ansatz can also be established through a very general approach, based on CP maps [see G. Chiribella and M. D'Ariano, quant-ph/0406237 (2004), and forthcoming papers].
  - [32] N. J. Cerf, *Phys. Rev. Lett.* **84**, 4497 (2000).
  - [33] N. J. Cerf, *J. Mod. Opt.* **47**, 187 (2000); *Acta Phys. Slovaca* **48**, 115 (1998).
  - [34] T. Durt and B. Nagler, *Phys. Rev. A*, **68**, 042323 (2003).
  - [35] V. Buzek and M. Hillery, *Phys. Rev. Lett.* **81**, 5003 (1998).
  - [36] R.F. Werner, *Phys. Rev. A* **58**, 1827 (1998).
  - [37] V. Buzek, S. Braunstein, M. Hillery and D. Bruss, *Phys. Rev. A* **56**, 3446 (1997).
  - [38] M. D'Ariano and C. Macchiavello, *Phys. Rev. A* **67**, 042306 (2003).
  - [39] F. Buscemi, G. M. D'Ariano, and C. Macchiavello, e-print quant-ph/0407103 (2004).